Internet Storm Center

isc.sans.edu/diary/29740

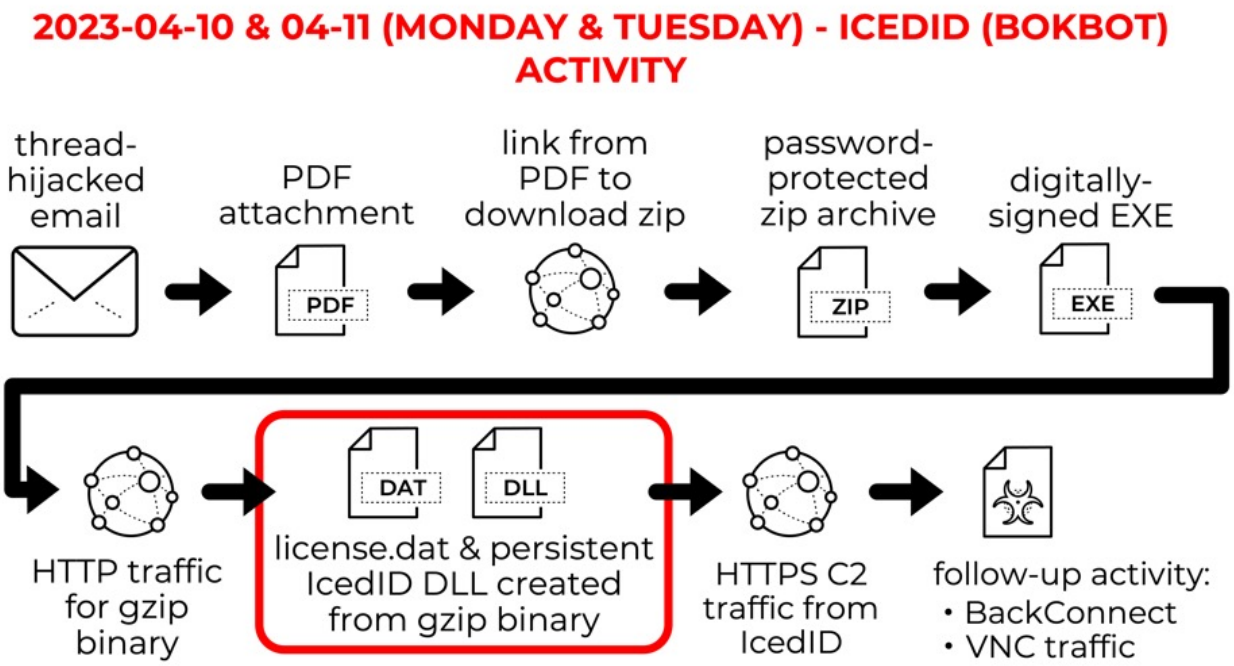
Recent IcedID (Bokbot) activity

Published: 2023-04-12
Last Updated: 2023-04-12 06:34:56 UTC
by Brad Duncan (Version: 1)
0 comment(s)

Introduction

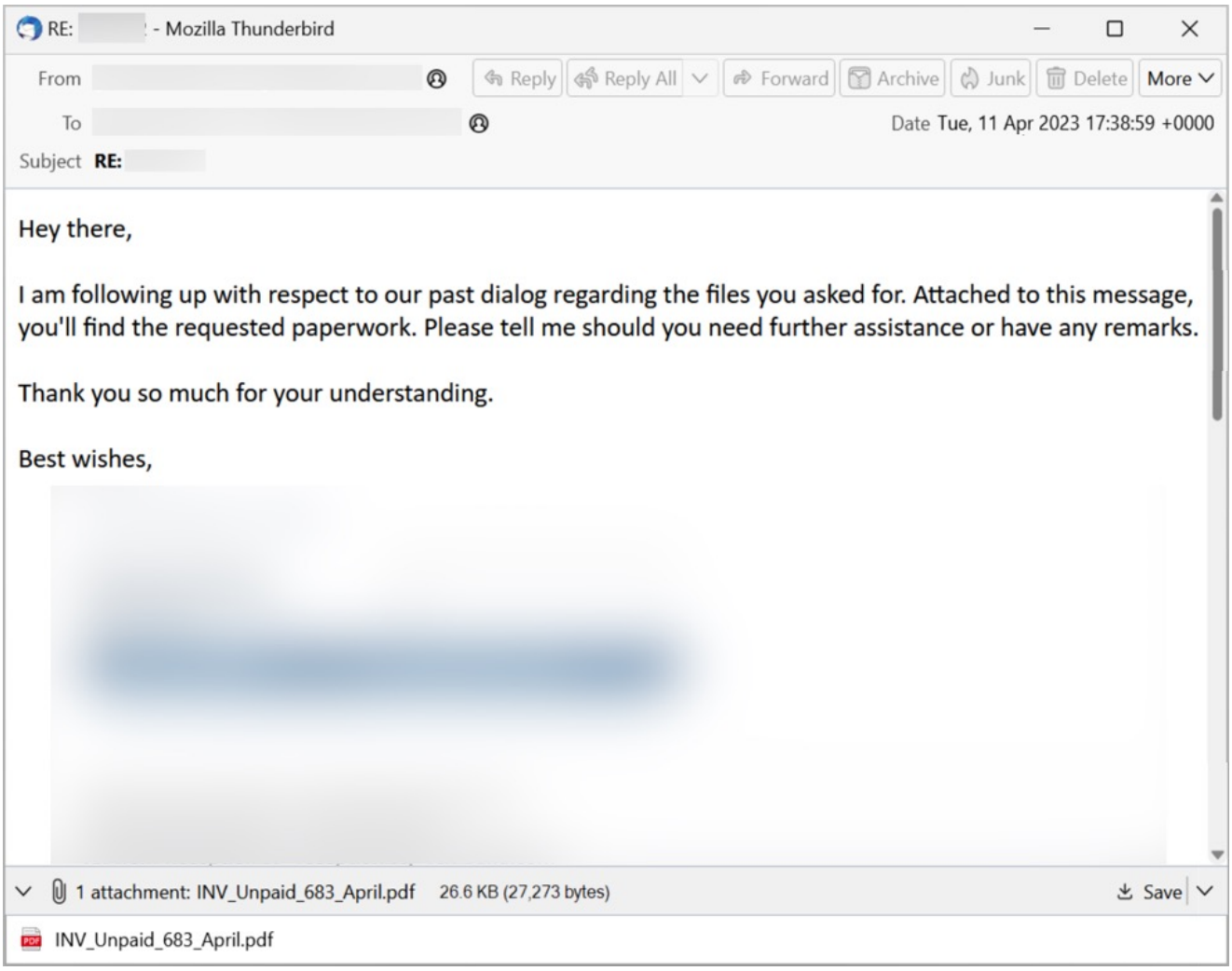
This week, we've seen IcedID (Bokbot) distributed through thread-hijacked emails with PDF attachments. The PDF files have links that redirect to Google Firebase Storage URLs hosting password-protected zip archives. The password for the downloaded zip archive is shown in the PDF file. The downloaded zip archives contain EXE files that are digitally-signed using a certificate issued by SSL.com. The EXE file is designed to install IcedID malware on a vulnerable Windows host.

Today's diary reviews an IcedID infection generated on Tuesday 2023-04-11.

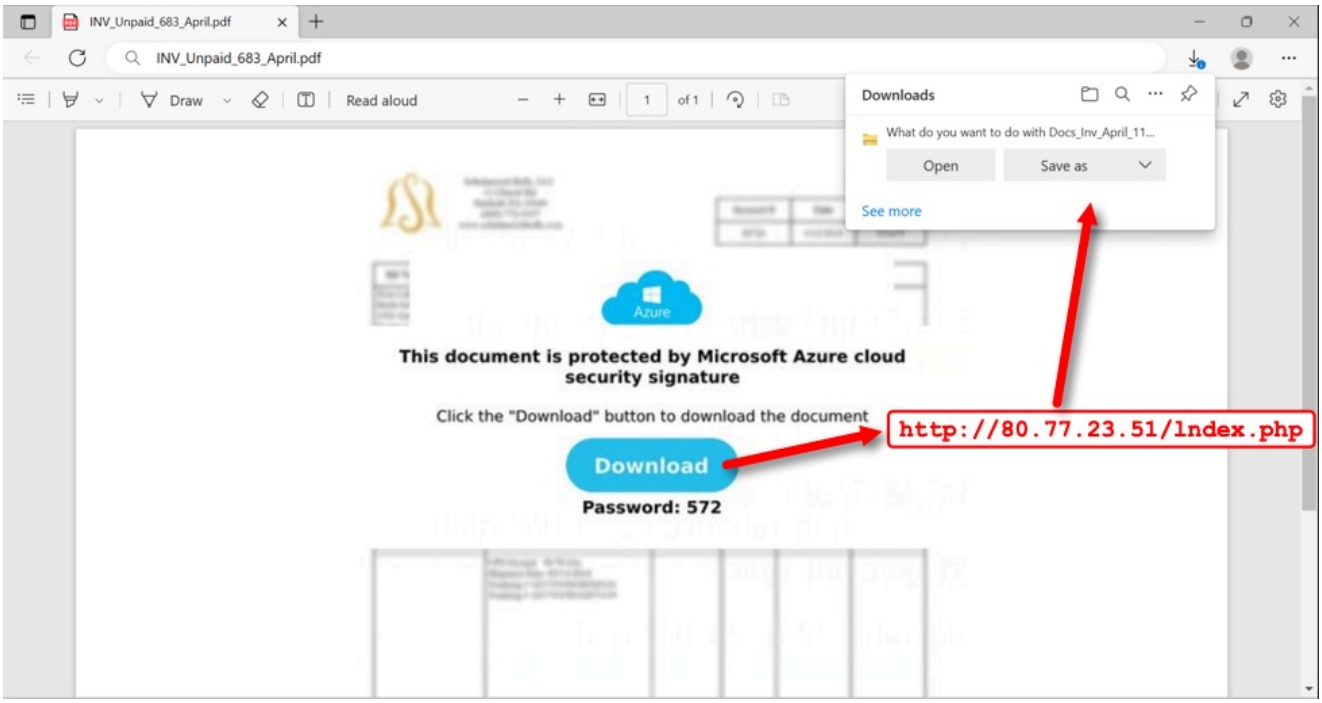


Shown above: Chain of events for IcedID infections so far this week.

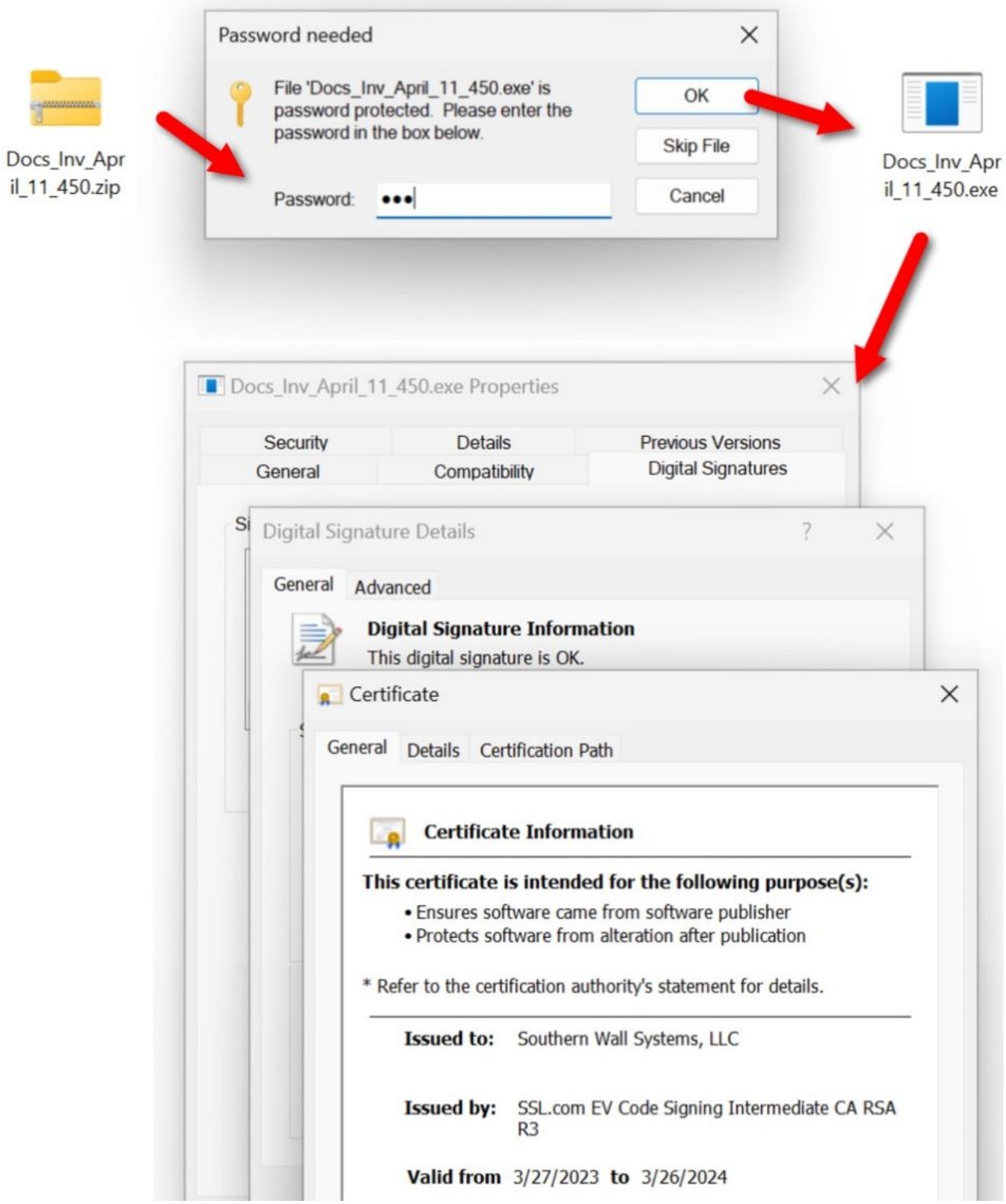
Images from the infection



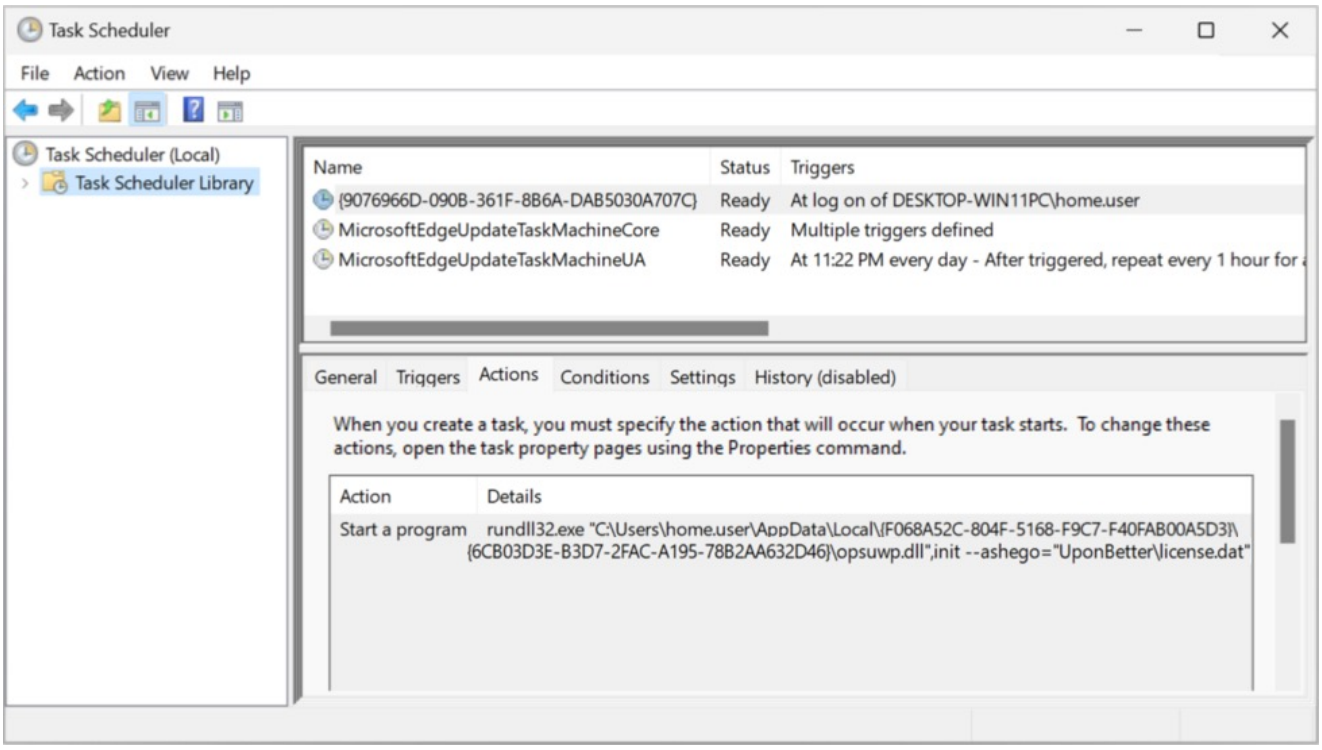
Shown above: Example of thread-hijacked email pushing IcedID from Tuesday 2023-04-11.



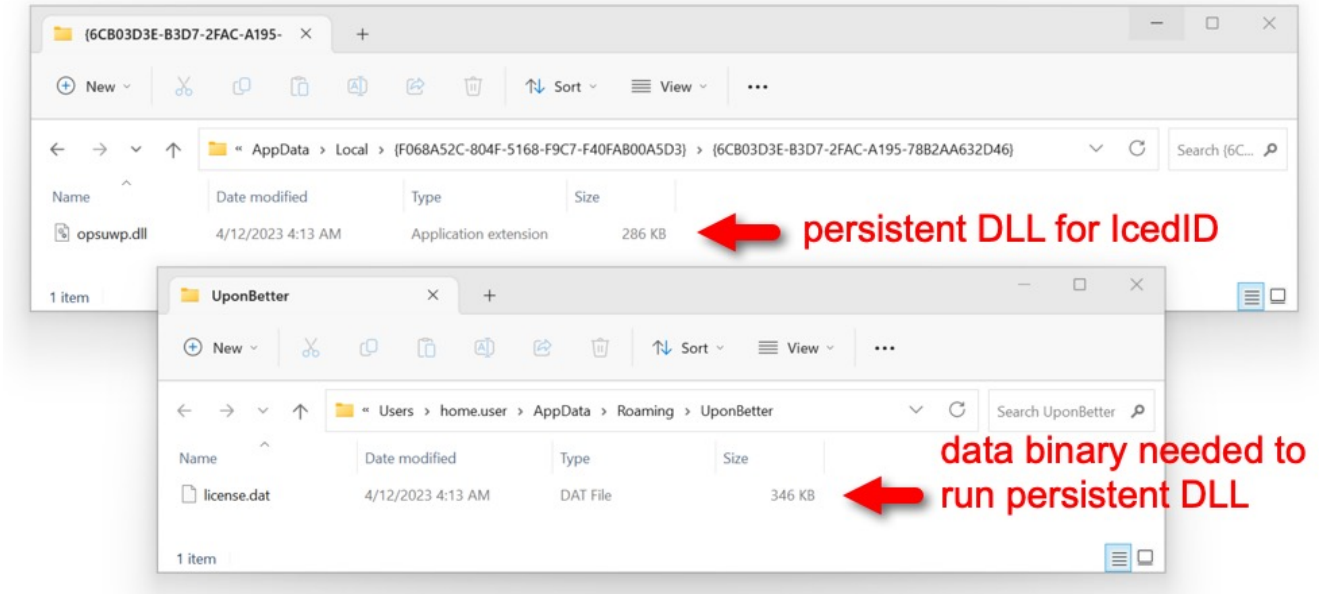
Shown above: Attached to the email, this PDF file has a link to download a password-protected zip archive.



Shown above: EXE extracted from the zip archive is digitally signed using a certificate issued by SSL.com.



Shown above: Scheduled task to keep the IcedID infection persistent.



Shown above: Persistent DLL for IcedID and the data binary used to run the persistent DLL.

Time	Dst	port	Host	Info
2023-04-12 03:56:15	80.77.23.51	80	80.77.23.51	GET /lndex.php HTTP/1.1
2023-04-12 03:56:17	142.250.68.138	443	firebasestorage.googleapis.com	Client Hello
2023-04-12 04:01:57	54.160.174.51	80	www.ssl.com	GET /repository/SSLcom-R
2023-04-12 04:13:28	172.86.75.64	80	shoterqana.com	GET / HTTP/1.1
2023-04-12 04:14:37	192.153.57.82	443	villageskaier.com	Client Hello
2023-04-12 04:14:39	192.153.57.82	443	villageskaier.com	Client Hello
2023-04-12 04:14:39	192.153.57.82	443	villageskaier.com	Client Hello
2023-04-12 04:14:40	162.33.178.40	443	deadwinston.com	Client Hello
2023-04-12 04:19:38	162.33.178.40	443	deadwinston.com	Client Hello
2023-04-12 04:24:40	162.33.178.40	443	deadwinston.com	Client Hello
2023-04-12 04:29:42	162.33.178.40	443	deadwinston.com	Client Hello
2023-04-12 04:34:43	162.33.178.40	443	deadwinston.com	Client Hello

Shown above: Traffic from the infection filtered in Wireshark.

Files From an Infected Windows Host

SHA256 hash:
6d07c2e05e76dd17f1871c206e92f08b69c5a7804d646e5f1e943a169a8c50ee

- File size: 27,273 bytes
- File name: INV_Unpaid_683_April.pdf
- File description: PDF file attached to thread-hijacked email distributing IcedID

SHA256 hash: 59e0f6e9c4ce2ab8116049d59525c6391598f2def4125515d86b61822926784f

- File size: 58,031 bytes
- File name: Docs_Inv_April_11_450.zip
- File location: hxxps://firebasestorage.googleapis[.]com/v0/b/logical-waters-377622.appspot.com/o/MCRERY0iJA%2FDocs_Inv_April_11_450.zip?alt=media&token=799ca8a7-44ce-44e8-b93d-a346faaf0ea3
- File description: password-protected zip archive downloaded from link in above PDF file
- Password: 572

SHA256 hash: 52d3dd78d3f1a14e18d0689ed8c5b43372f9e76401ef1ff68522575e6251d2cf

- File size: 131,168 bytes
- File name: Docs_Inv_April_11_450.exe
- File description: Extracted from the above zip archive, a 64-bit, digitally-signed EXE to install IcedID

SHA256 hash:
54d064799115f302a66220b3d0920c1158608a5ba76277666c4ac532b53e855f

- File size: 647,389 bytes
- File description: Gzip binary from shoterqana[.]com retreived by above EXE

SHA256 hash: dbf233743eb74ab66af8d1c803f53b7fe313ed70756efcc795ea4082c2f3c0c8

- File size: 354,282 bytes
- File location: C:\Users*[username]*\AppData\Roaming*[random directory name]*\license.dat
- File description: data binary used to run persistent IcedID DLL

SHA256 hash: 5953f8f23092714626427316dd66ff2e160f03d2c57dcb1a4745d2e593c907ae

- File size: 292,352 bytes
- File location: C:\Users*[username]*\AppData*[random directory path under Local or Roaming]**[random name]*.dll
- File description: Persistent IcedID DLL (64-bit DLL)
- Run method: rundll32.exe *[file name]*,init --ashego="*[path to license.dat]*"

Traffic From an Infected Windows Host

Link from the PDF file:

> hxxp://80.77.23[.]51/Index.php

Above URL redirected to:

> hxxps://firebasestorage.googleapis[.]com/v0/b/logical-waters-377622.appspot.com/o/MCRERY0iJA%2FDocs_Inv_April_11_450.zip?alt=media&token=799ca8a7-44ce-44e8-b93d-a346faaf0ea3

Caused when running the extracted EXE, because the EXE was digitally signed using a certificate from SSL.com:

- hxxp://www.ssl[.]com/repository/SSLcom-RootCA-EV-RSA-4096-R2.crt
- Note: The above URL is not malicious, but it's an indicator for this particular infection chain.

Installer EXE for IcedID retrieves gzip binary:

> 172.86.75[.]64 port 80 - shoterqana[.]com - GET / HTTP/1.1

IcedID C2:

- 192.153.57[.]82 port 443 - villageskaier[.]com - HTTPS traffic
- 162.33.178[.]40 port 443 - deadwinston[.]com - HTTPS traffic

Final words

Running recent IcedID samples in a lab environment this week generated IcedID BackConnect traffic over 45.61.137[.]159 over TCP port 443 (reference) and 193.149.176[.]100, also using TCP port 443 (reference). 443 is a new TCP port for IcedID

BackConnect traffic, which previously used TCP port 8080. These two IP addresses are good indicators of an on-going IcedID infection if you find traffic to these servers from your network.

Brad Duncan
brad [at] malware-traffic-analysis.net

Keywords: Bokbot IcedID malspam PDF
0 comment(s)

Comments

Login here to join the discussion.

Top of page
×

Diary Archives